Child Maintenance Service (DWP)

Data protection audit report

March 2022

Information Commissioner's Office

Executive summary

Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits.

The ICO is an independent, proportionate regulator and sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach. High standards of personal data protection compliance help organisations innovate and deliver great services by building trust with the public. The ICO's expertise and consistent approach to regulation provides certainty enabling organisations to feel confident to use personal data responsibly, innovate and support economic growth.

The ICO Civil Investigations Team made a referral to the ICO Assurance Team asking it to complete an audit of the Child Maintenance Service (CMS) which is part of the Department for Work and Pensions (DPW). The audit was to ensure that CMS had the correct measures in place around the processing of personal data, principally around the accuracy of records, security, disclosures and the reporting of personal data breaches. CMS and DWP agreed to a consensual audit of its processing of personal data, it polices and control measures.

The purpose of the audit is to provide the Information Commissioner, CMS and DWP with an independent assurance of the extent to which CMS, within the scope of this agreed audit, is complying with data protection legislation.

The scope of this audit was determined following a risk based analysis of CMS processing of personal data. The scope may take into account any data protection issues or risks which are specific to CMS identified from ICO intelligence or CMS' own concerns, and/or any data protection issues or risks which affect their specific sector or organisations more widely. The ICO has further tailored the controls covered in each scope area to take into account the organisational structure of CMS, the nature and extent of CMS' processing of personal data, and to avoid duplication across scope areas. As such, the scope of this audit is unique to CMS.

Audits are conducted following the Information Commissioner's data protection audit methodology. The key elements of this are normally a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

However, due to the outbreak of Covid -19, and the resulting restrictions on travel, this methodology was no longer appropriate. Therefore CMS agreed to continue with the audit on a remote basis. A desk based review of selected policies and procedures and remote telephone interviews were conducted from 7 February to 22 February 2022. The ICO would like to thank CMS for its flexibility and commitment to the audit during difficult and challenging circumstances.

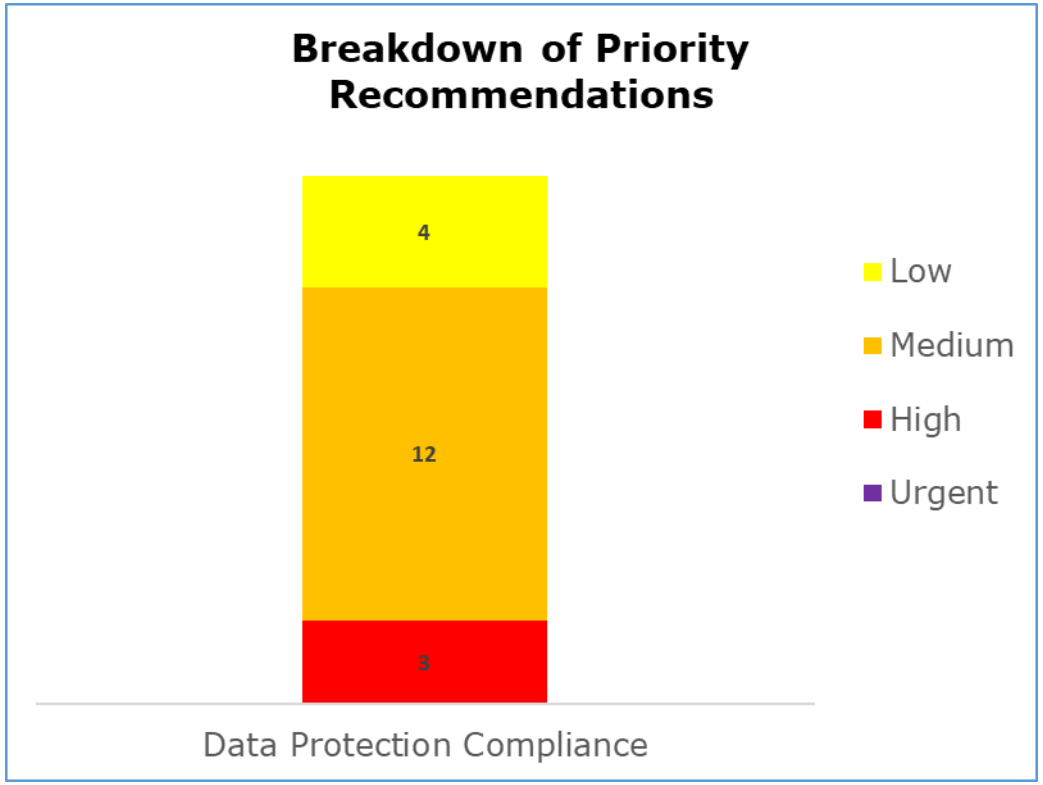
Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist CMS in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. CMS' priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope area	Assurance Rating	Overall Opinion
Data Protection Compliance	Reasonable	There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

*The assurance ratings above are reflective of the remote audit methodology deployed at this time and the rating may not necessarily represent a comprehensive assessment of compliance.

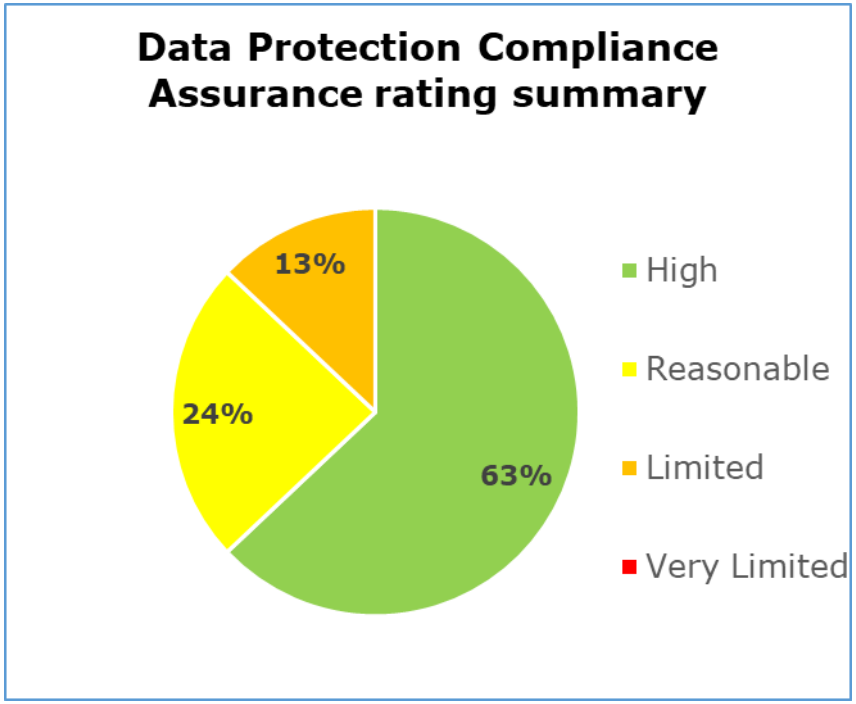
Priority Recommendations



The bar chart above shows a breakdown of the priorities assigned to our recommendations made:

- The audit conclusion resulted in three high, twelve medium and four low priority recommendations being made.

Graphs and Charts



The pie chart above shows a summary of the assurance ratings awarded across the audit scope. 63% high assurance, 24% reasonable assurance, 13% limited assurance, 0% very limited assurance.

Areas for Improvement

There are currently no formal central checks carried out to ensure business areas are complying with retention periods. Sample checks should be carried out by the Information Management and Compliance Team to ensure business areas are in compliance. Checks should be recorded and reported back to Data Protection Governance Board (DPGB).

Some staff data and minimal customer data is held in secure shared folders. Whilst staff confirmed that weeding of these records is carried out by managers, there are no local compliance checks to ensure the task has been carried out and data has been deleted in line with expected retention periods. Periodic checks should carried out by the Child Maintenance Group (CMG) and be recorded and reported back to Information Asset Managers (IAMs).

Further strengthening of procedures and guidance is required to ensure that all personal data breaches which meet the criteria of reporting to the ICO are reported within the required timeframe.

Best Practice

DWP has ensured a deliberate line management separation exists between its Data Protection (DP) and Information Security (IS) advisory and compliance functions and its operational functions. IS and DP sit within the Finance Group. This helps to minimise the risk of any conflict of interests.

DWP provides a refresher for training, including DP training three months after the initial induction, as staff receive a large amount of information when they commence employment and may have forgotten some in consequence.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of Child Maintenance Service and DWP.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of Child Maintenance Service and DWP. The scope areas and controls covered by the audit have been tailored to Child Maintenance Service and DWP and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.